June 2003

OSD(HA), TMA, TMI&S

Highlights

- HIPAA Overview
- HIPAA Security Rule
- Synopsis
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Security and Privacy

Information Assurance Program Office

Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA
22041-3206
Ph: 703-681-8786
Fax: 703-681-8814

For More Information:
www.tricare.osd.mil/imtr/default.htm

TMA HIPAA Website:
www.tricare.osd.mil/hipaa

E-Mail:
hipaamail@tma.osd.mil

TRICARE Management Activity

HIPAA – SECURITY

TRICARE Management Activity, Information Assurance Program Office

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

HIPAA Overview

As a result of the enactment of HIPAA, healthcare entities in the United States will be required to substantially alter the way they transmit and protect the medical records of their patients and members. In general terms, HIPAA is not a voluntary initiative but is a mandate to protect the confidentiality, integrity, and availability of individual health information.

HIPAA contains three sets of administrative simplification standards (transactions and code sets, privacy and security, and unique health identifiers). The rules governing transactions and code sets, privacy, and national employer identifier have been finalized and published. The Rule for a national provider identifier has been proposed and is under review. Rules for a national health plan identifier and unique individual health identifier have been discussed but not proposed. The final security rule was published in the Federal Register on February 20, 2003 and becomes effective April 21, 2003. Covered entities will have 26 months to become compliant, establishing the April 21, 2005 compliance date. Small health plans will have an additional year (April21, 2006).

HIPAA compliance begins at the organizational level, and in recognition of this the three Services have committed to having each Military Treatment Facility (MTF) form an interdisciplinary team, the Medical Information Security Readiness Team (MISRT).

MISRTs have been trained on the HIPAA Security WIPT endorsed risk assessment tool (Operationally Critical Threat Asset and Vulnerability Evaluation^{sm} (OCTAVE^{sm})) and are completing their facility assessments. OCTAVE^{SM} assessments are being completed in support of the April 14, 2003 HIPAA Privacy Rule Implementation date.

HIPAA Final Security Rule

The final HIPAA security rule adopts standards for the security of individually identifiable health information that is maintained, transmitted, or received in electronic form. Covered entities (health plans, health care clearinghouses, and certain health care providers) must comply with the rule by April 21, 2005 and small health plans must comply one year later (April 21, 2006). With the publication of the final security rule, covered entities must assure their patients that the integrity, confidentiality and availability of their protected health information (PHI) is secure. The security rule is comprised of three areas:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

The final rule includes several standards as well as implementation specifications which provide instructions for implementing those standards. Each implementation specification will be listed as “mandatory” or “addressable” and the covered entity must act accordingly. Addressable implementation specifications are included in the final rule to provide covered entities additional flexibility with respect to compliance with the security standards. These implementation specifications need to be looked at as part of the covered entities’ security management process and implemented or not based on the results of the security risk assessment. If a covered entity chooses not to implement either an addressable implementation specification or an alternative security measure, the covered entity must document the decision as well as the rationale behind that decision, and how the standard will be met.. The Golden Rule is you *must document everything*! What is documented must reflect what you actually do and it must be kept current and accurate.

Synopsis

The Defense Health Information Assurance Program and its Policies, Procedures, and Practices (P3) Work Group have been working steadily to assess HIPAA's impact and comparability to current DoD and Service regulations. They have developed tools, provided basic OCTAVE[sm] training and ensured advanced training is available to support the MISRTs. The membership has laid the groundwork for the MHS Security Working Integrated Project Team (WIPT) to plan the implementation.

In a nutshell, the final HIPAA security rule delineates administrative requirements and supporting implementation features. Security management principles and broad management controls are emphasized as the primary means for protecting patient health information. The final rule requires that procedures be documented, periodically reviewed and made available to individuals responsible for implementing the procedures or content. It also allows some flexibility in how it is implemented but requires the rationale for any deviation to be documented.

Administrative Safeguards

Administrative Safeguards are administrative actions and policies and procedures to manage the development and implementation of security measures to protect individually identifiable health information that is electronically maintained, transmitted, and/or received.
Of the eighteen major requirements dictated in the rule, half are in this section of the final rule. Some of the standards included in the Administrative Safeguards, are: *security management process, information access management, and security awareness and training.* In order to be HIPAA compliant, information security must involve all of the ways that people handle and access the information found in the information technology systems.

Physical Safeguards

Physical Safeguards involves the use of administrative measures and other mechanisms to control physical access to computer systems and facilities. It's focus is on protecting buildings, computer rooms and computer hardware from the threats of fire and other natural and environmental hazards, intrusion, and physical destruction or damage by humans. There exists some overlap with the Administrative Procedures category, however, Physical Safeguards emphasizes the facility and the physical security aspects of those procedures.

Technical Safeguards

In the final rule, Technical Security Services & Technical Security Mechanisms are combined to form "Technical Safeguards". Technical Safeguards differ from Administrative and Physical Safeguards as they generally function as security controls dealing with automated information systems. The proposed rule required encryption of electronic PHI transmitted over open networks. The final rule makes encryption of electronic PHI during transmission an addressable implementation specification.

Security and Privacy

Security and privacy are always linked together as the protection of the privacy of information depends on security measures to protect that information. The final privacy rule focuses on how a patient's PHI should be handled by mandating what uses and disclosures are authorized and what rights patients have with regard to their health information. The final security rule on the other hand, defines the administrative, physical, and technical safeguards to protect PHI. Whereas the privacy rule applies to PHI in any form, the security rule is more limited in that it applies only to PHI in electronic form.